CREST Certified Tester (CCT) examination – Sample Scenario

This document provides some useful and sample information related to CREST Certified Tester (CCT) examination when it comes to the Scenario component. It has been designed to give candidates an understanding of the structure of the Scenario component of the CCT examinations. It is not intended to replicate the scenario exam component in its entirety.

Candidates should use this to aid examination preparation, but should not use this as an indication of the technical content and capability required. Candidates should refer to the syllabus to understand the breadth and depth of the required knowledge and capability.

The following sections provide a breakdown of the Scenario Structure.

Scenario Overview

Candidates will be firstly presented with background information about the scenario, their role and what is expected from them.

Example:

You are a cyber security consultant working for a penetration testing organisation, specialising in providing penetration testing and consultancy services to various businesses across the globe.

You have been contracted by XYZ Inc., a multinational corporation, to undertake a comprehensive penetration test of their internal network. XYZ Inc. are a leading manufacturer of cutting-edge home appliance devices with a significant focus on protecting their intellectual property. The company operates offices in numerous countries around the world, making their internal network a crucial asset for their global operations.

XYZ Inc. are particularly concerned about ***the security of their intellectual property and the potential risks associated with unauthorised access to their proprietary information****.*

This is the primary driver behind their reasoning for penetration tests.

Following the scenario overview, candidates will be presented with questions and supporting evidence containing relevant information that will enable them to answer each question.

Scoping Phase (26 Marks)

Example:

After an initial meeting with XYZ Inc., a scoping questionnaire has been provided as part of the standard process. The purpose of the questionnaire is to correctly scope the assessment with the help of the client.

This has been completed by the customer. The key components of the engagement were discussed on a scoping call and XYZ Inc. provided their main areas of concern in a spreadsheet.

As the lead consultant on the assessment, it is your job to review the scope prior to the assessment starting.

Reporting Phase (30 Marks)

Example:

A security assessment has recently been completed for XYZ Inc. As the lead consultant, you are now tasked with writing or carrying out a quality review on the components that will compose the final report. The questions include supplemental information in the form of basic reports and tool output.

Candidates will then be asked to:

- Write or QA a Management summary
- Write or QA a Technical summary

Issue Write up (30 Marks)

Using a supplied risk ratings table, candidates will be provided with access to raw evidence from the assessment. Utilising the evidence provided, candidates are required to write up one of two possible issues presented in their respective scenario.

Legal and compliance (4 Marks)

Based on their local or operating jurisdiction, candidates will need to consider legal, compliance and ethical consequences related to the scenario presented.

Scenario Example Evidence

Candidates will be presented with pieces of evidence alongside each question. Some examples of what the evidence could look like in the exam are provided below.

Primary Concerns

This is an example of a primary concerns table including client's inputs and relevant information regarding risks and priority level.

Risk	Priority	Notes
Access to critical ORACLE DATABASE servers and the intellectual property contained within.	HIGH	The business IP is stored in these servers so gaining access to this via User LAN is a high risk
Availability of critical servers for legitimate activities during working hours.	HIGH	Especially Database Servers
Lateral movement between networks.	HIGH	Specifcally User LAN to Corporate LAN
User password hygiene and security awareness.	MEDIUM	Ensure users are not storing passwords anywhere other than dedicated password managers
Mobile Devices and their ability to exfiltrate corporate data out of the secure environment.	MEDIUM	Ensure users are not using their personal devices to connect to the network. Ensure users are not able to connect their personal devices to the corporate WiFi

Scenario Scoping Questionnaire

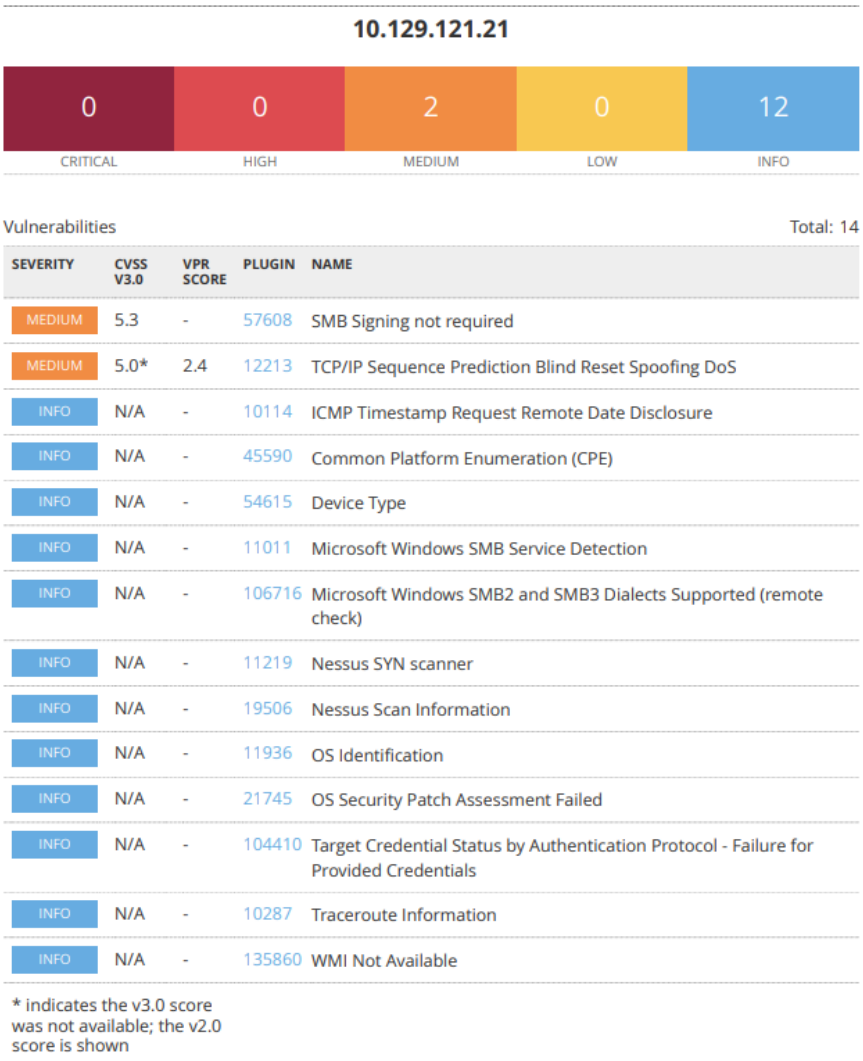
This is an example of a Scoping Questionnaire provided by the client and that needs to be reviewed by the candidate as part of the QA.

CYBERGUARD SOLUTIONS INTERNAL PENETRATION TEST SCOPE DOCUMENT		
Item	Response	Notes
DHCP or Manual Network Configuration?	Manual Network Configuration	IP Address: 10.15.10.10-15 Netmask: 255.255.255.0. Gateway: 10.15.10.254
Network ranges to be assessed:	10.0.30.0/24 10.15.10.0/24 172.36.10.0/24	Two main internal networks
How many Windows Servers?	9	6x Windows Server 2019 3x Windows Server 2008 R2 ECOORADBS003 ECOORADBS002
How many Unix / Linux Servers?	13	
How many Laptops / Desktops in scope?	~ 40 Laptops ~ 20 Desktops	
Are the servers to be build reviewed, gold image reviewed also ?	Yes	
Are there any end user devices in scope of the assessment?	Yes, users have laptops and mobile phone devices	Unknown how many devices in total
How many mobile devices are in scope ?	~ 40 mobile devices	
Out of scope devices	10.0.30.2 Database Server - 172.31.10.18 Any devices labelled ECOORADBPRD* (Production Oracle Databases)	Database server is out of scope due to being critical service within EcoFusion. This holds proprietary data
Are all the in scope items owned and property of EcoFusion Inc. ?	No	The 172.36.10.0/24 range is owned and operated by SecureHosting Limited.

Tool Outputs

Some tool outputs will also be provided to support candidates with the report writing elements of the scenario. A few examples are provided below:

Nessus Output



10.129.121.21

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	0	12

Vulnerabilities — Total: 14

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.0*	2.4	12213	TCP/IP Sequence Prediction Blind Reset Spoofing DoS
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	21745	OS Security Patch Assessment Failed
INFO	N/A	-	104410	Target Credential Status by Authentication Protocol - Failure for Provided Credentials
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	135860	WMI Not Available

* indicates the v3.0 score was not available; the v2.0 score is shown

MSFConsole SNMP Output

```
msf6 auxiliary(scanner/snmp/snmp_login) > set RHOSTS 10.129.121.1-10
RHOSTS => 10.129.121.1-10
msf6 auxiliary(scanner/snmp/snmp_login) > run

[*] Scanned  1 of 10 hosts (10% complete)
[*] Scanned  2 of 10 hosts (20% complete)
[*] Scanned  3 of 10 hosts (30% complete)
[*] Scanned  4 of 10 hosts (40% complete)
[+] 10.129.121.5:161 - Login Successful: public (Access level: read-write); Proof (sysDescr.0): Linux nxcluster_ 2.4.21-50.EL #1 SMP Tue May 8 17:10:00 EDT 2007 x86_64
[*] Scanned  5 of 10 hosts (50% complete)
[*] Scanned  6 of 10 hosts (60% complete)
[*] Scanned  7 of 10 hosts (70% complete)
[*] Scanned  8 of 10 hosts (80% complete)
[*] Scanned  9 of 10 hosts (90% complete)
[*] Scanned 10 of 10 hosts (100% complete)
[*] Auxiliary module execution completed
```